

ABSTRACT

Methods and apparatus for the generation of a cryptographic one way function (a key or keystream generator) for use in encrypting or decrypting binary data. A non-linear key or keystream generation algorithm using multiple feedback shift registers is provided. The feedback shift registers may be constructed utilizing an advanced mathematical construct called an extended Galois Field GF(2^m). The key or keystream is generated as a non-linear function of the outputs of the multiple feedback shift registers, which may be a combination of static feedback shift registers and dynamic feedback shift registers. Dense primitive polynomials with many coefficients may be used to produce a cryptographically robust keystream for use as an encryption or decryption key.